UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

FERROVIAL CONSTRUCTION US CORP. and NORTH PERIMETER CONTRACTORS, LLC,	:	CIV. NO. _____
Plaintiffs,	:	JUDGE _____
VERSUS	:	
JESUS GONZALEZ FERNANDEZ.	:	MAGISTRATE _____
Defendants.	:	

VERIFIED COMPLAINT FOR INJUNCTIVE RELIEF AND DAMAGES

Plaintiffs, Ferrovial Construction US Corp. ("FCUS") and North Perimeter Contractors, LLC ("NPC," and collectively with FCUS, "Plaintiffs") respectfully file this *Verified Complaint for Injunctive Relief and Damages*. This action arises out of the theft of trade secrets by Defendant, Jesus Gonzalez Fernandez ("Gonzalez"). Plaintiffs bring this action under the Defend Trade Secrets Act, 18 U.S.C. § 1125 *et seq.* ("DTSA"), and the Georgia Trade Secrets Act, O.C.G.A. § 10-1-760 *et seq.* ("GUTSA").

NATURE OF THE CASE

1. Plaintiffs have recently uncovered a scheme by Gonzalez to steal Plaintiffs' trade secrets in order to unfairly compete on behalf of Plaintiffs' competitor, Acciona, S.A., and its subsidiaries (collectively, "Acciona").

2. Plaintiffs are part of the corporate family of businesses whose ultimate parent is Ferrovial SE ("Ferrovial"), which is internationally recognized for its unique ability to design and develop large-scale transportation infrastructure projects. FCUS is focused on design-build projects throughout North America, and NPC, its subsidiary, is a special purpose entity formed to

complete the Transform 285/400 design-build-finance project at the interchange of I-285 and SR400 (the "285/400 Project").

3. For his part, Gonzalez has worked within the Ferrovial family of companies for nearly two decades and, since 2016, has performed work for NPC as a Project Design Manager, entrusted with the management and completion of design services performed in connection with the 285/400 Project. Gonzalez also performed design management services for FCUS in its pursuit of major, billion-dollar procurements in Georgia. In these roles, Gonzalez had access to Plaintiffs' trade secrets and was obligated—through various corporate policies—to use those trade secrets for Plaintiffs' exclusive benefit. That is, Gonzalez was strictly prohibited from converting Plaintiffs' trade secrets for his own benefit or the benefit of a competitor like Acciona.

4. On November 19, 2024, Gonzalez unexpectedly submitted his resignation notice, which came as a shock given his long tenure within the Ferrovial family of businesses and his recent introduction as a potential "Design Manager" for an upcoming infrastructure project. Even more shocking, however, was what Gonzalez did in preparation for his departure. He downloaded over 100,000 documents from Plaintiffs' password-protected computing network, many of which contain and comprise Plaintiffs' trade secrets, including but not limited to: engineering drawings, construction strategies, design management plans, bids and bidding strategies, project risk summaries, and pricing information.

5. Plaintiffs were not aware of this fact until they started an investigation, which resulted in an alert from their internal cybersecurity team about potentially suspicious computing activity on Gonzalez's work computer. The initial results of this internal investigation were

alarming and prompted Plaintiffs to retain outside legal counsel as well as computer forensic experts.

6. The legal and forensic investigation remains ongoing, and may implicate others, but as of now, Plaintiffs can confirm several alarming facts that necessitate the need for injunctive relief and further forensic examinations of all computing devices to which Gonzalez (and those acting in concert with Gonzalez) had access. Specifically alarming are four pieces of evidence: one, Gonzalez misappropriated trade secrets relating to projects on which he had no material involvement; two, Gonzalez misappropriated trade secrets relating to a multi-million-dollar project that is currently out for bid and that Gonzalez's new employer, one of Acciona's subsidiaries, is also bidding on; three, Gonzalez tried to hide some of the most egregious activity by removing highly concerning folders from an external storage device that he returned following a demand from Plaintiffs' legal counsel; and four, Gonzalez failed to return at least three external storage devices that he plugged into his work computer shortly before resigning.

7. If Gonzalez is not enjoined—and, most critically, required to submit his computing devices to forensic examinations to enable purging the misappropriated information—Plaintiffs will face the threat of continued irreparable harm, as he (and potentially others) will continue to have improper access to a trove of Plaintiffs' trade secrets that can be used to compete unfairly.

PARTIES

8. Plaintiff Ferrovial Construction US Corp. is a corporation organized under the laws of Delaware, with its principal place of business in Texas.

9. Plaintiffs North Perimeter Contractors, LLC is organized under the laws of Delaware, whose member is a citizen of Georgia.

10. Defendant Jesus Gonzalez Fernandez is a citizen of Spain and is domiciled within this district.

JURISDICTION AND VENUE

11. The Court has subject matter jurisdiction over this matter under 28 U.S.C. § 1331 and § 1367. This case presents a claim arising under the laws of the United States, specifically the DTSA. The remaining state law claims are part of the same case and controversy as the DTSA claim.

12. The Court may exercise personal jurisdiction over Gonzalez, as he is domiciled in the State of Georgia. Additionally, these causes of action arise specifically out of his contacts with Georgia.

13. Venue is proper in the Northern District of Georgia under 28 U.S.C. § 1391, as a substantial part of the events giving rise to these claims occurred in this district.

FACTUAL BACKGROUND

Plaintiffs' Business and Its Trade Secrets

14. FCUS, as part of the Ferrovial family of corporate entities, operates as a leading contractor within the transport infrastructure industry by providing civil infrastructure solutions through its unique ability to leverage the engineering and construction expertise it has fostered across its family of businesses. FCUS performs design and construction of sustainable, innovative, and efficient infrastructure for governmental owners and for Ferrovial affiliates, which develop and operate such projects across the United States. The Greater Atlanta area is a key market for Ferrovial, and the prospective infrastructure projects within it are strategic targets.

15. Ferrovial operates through a family of corporate entities, many of which have specific responsibilities based on the individual needs of large-scale infrastructure projects. One such corporate entity is NPC, which is focused on the completion of an existing large-scale infrastructure project within the Atlanta-metro area.

16. A substantial part of the competitive position of Ferrovial and its family of businesses lies in their confidential business information. This information is one of their greatest assets. Accordingly, Ferrovial and its family of businesses (including NPC) take substantial care to keep this information out of its competitors' hands.

17. To protect this information, Plaintiffs require employees to agree to various employment policies and procedures designed to protect the information's confidentiality. For instance, employees must agree to be bound by a "Corporate Code of Ethics" that states: "Ferrovial's proprietary and confidential information is one of its greatest assets," which includes "[t]echnical information, designs, process data, pricing information, strategic plans, know-how, software and technology." It further states that employees "should never use Ferrovial's confidential information – or that of third parties – outside the scope of the professional context in which it was originally obtained" and that "Ferrovial's property should never be used for offensive or illegal purposes, conducting personal or other business, or to further the activities of a competitor."[1]

18. Employees also agree to be bound by a "Policy Guide," which prohibits the misuse of confidential business information;[2] the "Procedure for the Use of Technological Resources,"

[1] A true and correct copy of the "Corporate Code of Ethics" is attached as **Exhibit 1**.

[2] A true and correct copy of "Policy Guide" is attached as **Exhibit 2**.

which serves the purpose of "safeguarding the integrity, confidentiality, and availability of Ferrovial's information;[3] and the "Competition Policy," which specifically prohibits the exchange of confidential business information among competitors.[4] In fact, in order to log into his computer, Gonzalez (like all employees with access to the computing network of the Ferrovial family of businesses) was required to acknowledge and agree that access was limited for the purpose of performing work for Ferrovial family of companies and subject to compliance with the Procedure for the Use of Technological Resources.

19. Gonzalez was bound by these policies during his employment within the Ferrovial family of businesses, including when he was most recently employed by NPC.

20. Plaintiffs further protect their confidential information on password-protected internal computer servers that can only be accessed by select employees who have a valid reason to review or use the information. Several documents are further protected such that only certain management-level employees have the ability to modify sensitive data points within the documents. Plaintiffs also train their employees, including all new hires, with access to confidential company documents that the documents are confidential and valuable to Plaintiffs and should not be disclosed to anyone outside of the Ferrovial family of businesses. In fact, before Gonzalez could even log into his work computer to access Plaintiffs' computing network, Gonzalez was required to acknowledged that he understood he was bound by, and would abide by, Plaintiffs' policies restricting the use of their information.

[3] A true and correct copy of the "Procedure for the Use of Technological Resources" is attached as **Exhibit 3**.

[4] A true and correct copy of the "Competition Policy" is attached as **Exhibit 4**.

21. Additionally, Plaintiffs are able to monitor employees' computing activity and do so in order to safeguard their trade secrets.

22. Plaintiffs have instituted these measures because this information, in the hands of a competitor, can be used to compete unfairly and could cause irreparable harm.

Gonzalez Works within the Ferrovial Family of Businesses

23. Gonzalez started working within the Ferrovial family of businesses seventeen years ago. During that time, Gonzalez was provided a company-issued computer as well as access to a password-protected network that contained various trade secrets relating to past, current, and prospective projects that he may need to perform his duties.

24. Most recently, Gonzalez was assigned by Ferrovial to perform design management services for NPC on the 285/400 Project and for FCUS in its pursuit of certain infrastructure projects within the Greater Atlanta area.

25. However, during this time, there were other bids for prospective projects within the Greater Atlanta area that Gonzalez had no role in developing. Some examples were bids for the "SR400 Express Lanes Project" and "Sensitive Project No. 1."[5].

[5] To protect the commercially sensitive nature of this project, Plaintiffs have renamed it "Sensitive Project No. 1.

Gonzalez Unexpectedly Resigns to Join a Competitor, as do two other Key Personnel

26. During the summer of 2024, NPC was focused on completing the 285/400 Project but there were other infrastructure projects within the Greater Atlanta area that came up for bid: the "West Interchange Project" and the "SR400 Express Lanes Project."

27. Gonzalez was designated as the Proposal Design Manager on the "West Interchange Project," and that bid was submitted on June 12, 2024.

28. Shortly before this bid submission, on May 7, 2024, the bid for the "SR400 Express Lanes Project" was submitted, but Gonzalez was not materially involved in developing the design for the bid for the "SR400 Project." Rather, on that project, he participated in developing a design quality management plan and certain schedule items.

29. Both the "West Interchange Project" and the "SR400 Express Lanes Project" were subject to a competitive bid process. In fact, there were only two bidding consortiums on the "SR400 Express Lanes Project," and Acciona was a member of the competing team that submitted a bid on the SR400 Express Lanes Project.

30. From June 12, 2024, through August 14, 2024, while awaiting decisions on which bidding team would be awarded these two projects, various preparation meetings were convened to discuss plans if either one or both bids were won. Gonzalez participated in these meetings.

31. But, on August 15, 2024, Plaintiffs learned that the "SR400 Express Lanes Project" was awarded to the competing team, of which Acciona is a member.

32. Shortly thereafter, attention shifted to "Sensitive Project No. 1." Meetings began to be held about the strategy for bidding this project, including the possibility of involving Gonzalez

in the bidding process once he finished assigned tasks associated with the ongoing 285/400 Project that NPC was working to complete.

33. From late August through November 13, 2024, Gonzalez participated in internal strategy meetings about "Sensitive Project No. 1," and he also participated in meetings on November 13-14, 2024, with strategic business partners who would be involved in the bidding process.

34. Nevertheless, on November 19, 2024, Gonzalez unexpectedly submitted a resignation notice.

35. He had accepted a position with Acciona, which had been awarded the "SR400 Express Lanes Project," but prior to the resignation notice, Gonzalez had not disclosed that he was in talks with Acciona for potential employment.

Gonzalez Misappropriates Trove of Trade Secrets before Resigning

36. Around the time of Gonzalez's resignation notice, Plaintiffs' internal cybersecurity team alerted Plaintiffs about potentially suspicious computing activity from Gonzalez's computer.

37. Specifically, Plaintiffs' monitoring software indicated that there were mass transfers of documents from Plaintiffs' computing network to external storage devices plugged into Gonzalez's work-issued computer.

38. Plaintiffs conducted an internal investigation to further examine this activity and discovered alarming facts.

39. From late October 2024 through November 15, 2024 (*i.e.*, four days before his resignation notice), Gonzalez transferred nearly 100,000 documents from Plaintiffs' computing

network to external storage devices, including confidential business information relating to projects and bids in which Gonzalez was not materially involved.

40. For instance, on October 26, 2024, Gonzalez started transferring over ***10,000 documents***, several of which related to the bid for the "SR400 Express Lanes Project" that Gonzalez did not materially work on.

41. The same type of misconduct occurred in the days leading up to his unexpected resignation notice:

- October 27, 2024: Gonzalez transferred over ***18,000 documents***;
- October 28, 2024: Gonzalez transferred over ***11,700 documents***;
- October 29, 2024: Gonzalez transferred over ***6,600 documents***;
- October 30, 2024: Gonzalez transferred over ***13,200 documents***;
- November 4, 2024: Gonzalez transferred over ***7,800 documents***;
- November 5, 2024: Gonzalez transferred over ***12,100 documents***;
- November 6, 2024: Gonzalez transferred over ***14,800 documents***;
- November 7, 2024: Gonzalez transferred over ***7,400 documents***;
- November 8, 2024: Gonzalez transferred over ***400 documents***, including a .pst file (containing numerous emails) and documents relating to the "SR400 Express Lanes Project";
- November 11-12, 2024: Gonzalez transferred over ***40 documents***, some of which related to "Sensitive Project No. 1" that Gonzalez was not yet materially involved in;
- November 13, 2024: Gonzalez transferred over ***600 documents***;
- November 14, 2024: Gonzalez transferred more business-related documents; and

- November 15, 2024: Gonzalez transferred several .pst files (full of numerous emails), as well as files related to the "SR400 Express Lanes Project" that Gonzalez was not materially involved in.

42. Plaintiffs' discovery of this computing misconduct led to the hiring of computer forensic experts, who have independently confirmed the significant data migration from Plaintiffs' computing network to external storage devices that were plugged into Gonzalez's work-issued computer.

43. In addition, the reports on Gonzalez's computing activity even showed that Gonzalez was attending meetings with Plaintiffs' competitor—Acciona—regarding the "SR400 Express Lanes Project" before Gonzalez even notified Plaintiffs that he was resigning to join Acciona.

44. Further, forensics on external storage devices that Gonzalez returned in response to the demand of Plaintiffs' counsel indicated more alarming facts. For instance, Plaintiffs' internal monitoring reports indicated that Gonzalez had transferred folders that contain sensitive information to an external storage device, including folders titled "4. [Sensitive Project No. 2]"[6] on 10/28/2024 at 2:38 PM; "21 DSA TEMPLATES on 10/30/2024 at 5:02 AM; "22. DOWNLOADS FERRO LAPTOP" on 11/13/2024 at 2:30 PM; "23 CONTRATOS INGENIERIAS" on10/31/2024 at 3:05 PM; "Correo" on 11/7/2024 at 2:40 AM; "Jesus Correo" on 11/15/2024 at 12:14 PM; "13. [Sensitive Project No. 1]" on 11/12/2024 at 9:34 PM; and "22. DESKTOP FILES" on 11/14/2024 at 1:54:00 AM. However, when Gonzalez returned this external

[6] To protect the commercially sensitive nature of this project, Plaintiffs have renamed this folder "Sensitive Project No. 2."

storage device, those folders had been removed, which strongly indicates that Gonzalez had plugged the device into some other computer (*i.e.*, not his work computer) to remove those folders from the external storage device.

45. In other words, those folders are unaccounted for, and another computing device has been exposed to the misappropriated information. Gonzalez has not identified that device or provided that computing device for forensic examination.

46. Additionally, the forensics on Gonzalez's work computer also indicates that there are three unaccounted for external storage devices that Gonzalez plugged into his work computer shortly before resigning. These include (1) a WD Easystore 2624, last connected on 8/1/24 and last disconnected on 8/2/24; (2) a WD MyPassport 25EA, last connected on 10/26/24 and last disconnected 10/28/24); and (3) a Seagate BUP, last connected on 11/15/24 and last disconnected on 11/15/24.

Gonzalez Misappropriated Ferrovial's Playbook and Is Competing Unfairly

47. Stopping the harm following from and threatened by this data misappropriation is of tantamount importance because some of Plaintiffs' most critical business information is located within those misappropriated documents.

48. For instance, Gonzalez misappropriated engineering designs and stick diagrams relating to projects that comprise strategies for maximizing revenue on projects; internal communications comprising unique strategies for bidding these large-scale infrastructure projects; design quality management plans that contain Plaintiffs' proprietary design processes to establish overall design production, review, and implementation process that impacts pricing in numerous ways; various due diligence documents that reflect Plaintiffs bidding approach that reveals their

unique approach to bidding on projects; pricing documents that reflect a unique approach and strategy for bidding on large-scale projects; risk summaries and registers that set forth projected costs and contingencies and include forecasted opportunities for design optimization not fully fleshed out in the bid design, all of which reflects company principles that enhance Plaintiffs' competitive advantage; draft agreements and strategy comments contained therein; various pricing documents; and technical proposals.

49. Taken together, the misappropriated information essentially provides a competitor—like Gonzalez and Acciona—with the blueprints to strip or severely minimize Plaintiffs' competitive advantage. In the hands of a direct competitor, this information is devastating to Plaintiffs.

50. This is especially true considering that Gonzalez misappropriated information relating to projects that are not only still out for bid but also are being competitively bid on by his new employer, Acciona. In other words, through Gonzalez's (and possibly others') retention of this information and now current employment, Acciona would in turn have access to the misappropriated information.

51. Gonzalez, and all other individuals and entities acting in concert with him, must be enjoined from retaining, using, and disclosing the misappropriated trade secrets, and must submit their devices to a thorough computer forensic examination to ensure that Plaintiffs' information is permanently removed.

CAUSES OF ACTION

COUNT 1
Violation of the Defend Trade Secrets Act

52. Plaintiffs repeat and re-allege each of the allegations of the preceding paragraphs

as if fully stated here.

53. The DTSA defines a trade secret as, *inter alia*, "all forms and types of financial, business, scientific, technical, economic, or engineering information . . . whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing" provided that the owner took "reasonable measures to keep such information secret," and it offers the holder of the trade secret an advantage over competitors who do not use the trade secret.

54. Plaintiffs' trade secrets were kept secret by reasonable measures undertaken by Plaintiffs to protect the secret and private nature of the information.

55. Plaintiffs' trade secrets are related to products and services offered in interstate commerce.

56. Gonzalez was entrusted with this confidential business information in the performance of his work duties.

57. As detailed above, in the days and weeks before he ended his relationship with Plaintiffs, Gonzalez surreptitiously and improperly took these trade secrets and, at a minimum, is threatening to unlawfully use them to benefit himself and Acciona.

58. The categories of misappropriated Plaintiffs' information include: engineering designs and stick diagrams; internal communications comprising unique strategies for bidding these large-scale infrastructure projects; design quality management plans; various due diligence documents that reflect Plaintiffs' bidding approach that reveals their unique approach to bidding on projects; pricing documents; risk summaries and registers; draft agreements and strategy

comments contained therein; and various bidding documents and proposals.

59. As a direct result of Gonzalez's conduct, Plaintiffs are, at a minimum, facing the very real and significant risk of being irreparably harmed, as well as other damages.

COUNT 2
Violation of Georgia Trade Secrets Act

60. Plaintiffs repeat and re-allege each of the allegations of the preceding paragraphs as if fully stated here.

61. The Georgia Trade Secrets Act ("GTSA") is similar to the DTSA in terms of how it defines what constitutes a "trade secret" and a "misappropriation."

62. Under the GTSA, documents that Gonzalez downloaded from Plaintiffs' computing network qualify as "trade secrets," as they derive independent economic value from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from their disclosure or use. Further, these trade secrets have been the subject of reasonable effort to maintain their secrecy.

63. Gonzalez "misappropriated" these trade secrets within the meaning of O.C.G.A. § 10-1-761 by obtaining them without authorization and/or through improper means.

64. As a direct result of Gonzalez's conduct, Plaintiffs are, at a minimum, facing the very real and significant risk of being irreparably harmed, as well as other damages.

65. Gonzalez's misappropriation of Plaintiffs trade secrets is willful, wanton, reckless, and malicious, entitling Plaintiffs to an award of exemplary damages in an amount authorized by O.C.G.A. § 10-1-763(b).

66. Through O.C.G.A. § 10-1-764, Plaintiffs are entitled to an award of its attorneys' fees and costs incurred in this action because Gonzalez willfully and maliciously misappropriated

Plaintiffs' trade secrets, knowing them to be trade secrets.

JURY DEMAND

67. Plaintiffs demand a trial by jury.

PRAYER FOR RELIEF

For these reasons, Plaintiffs respectfully request Gonzalez be cited to appear and answer, and Plaintiffs respectfully request that the Court enter a judgment against Gonzalez awarding money damages and all other relief to which Plaintiffs are entitled in law and equity, including but not limited to:

1. After due proceedings conclude, entry of a preliminary injunction prohibiting Gonzalez, and/or any person or entity acting in concert with him, from using, disclosing, or disseminating Plaintiffs' trade secrets; and computer forensic examinations to ensure the remediation of Plaintiffs' trade secrets from the relevant devices and accounts.

2. After due proceedings conclude, entry of a permanent injunction, an award of damages based on all the claims stated herein (actual, compensatory, exemplary, and punitive), and other such damages as provided by applicable statute or common law, including attorneys' fees, expert fees, and costs. The permanent injunction shall prohibit Gonzalez, and/or any person or entity acting in concert with him, from using, disclosing, or disseminating Plaintiffs' trade secrets;

3. Judgment in favor of Plaintiffs and against Gonzalez on all counts, awarding all compensatory, exemplary, and punitive damages to which Plaintiffs are entitled;

4. An award of Plaintiffs' reasonable attorneys' fees and costs incurred in pursuing the counts set forth above; and

5. Any and all other relief this Court deems just, proper, equitable, and necessary under the circumstances.

Respectfully submitted:

/s/Chad V. Theriot

Chad V. Theriot
JONES WALKER LLP
3455 Peachtree Road NE, Suite 1400
Atlanta, GA 30326
Telephone: 404-870-7515
Email: ctheriot@joneswalker.com

and

*Joseph F. Lavigne (La. Bar No. 28119)
*P.J. Kee (La. Bar No. 34860)
JONES WALKER, LLP
201 St. Charles Avenue - 50th Floor
New Orleans, Louisiana 70170-5100
Telephone: (504) 582-8000
Facsimile: (504) 589-8610
Email: jlavigne@joneswalker.com
Email: pkee@joneswalker.com
*Pro Hac Motions To Be Filed

Counsel for Plaintiffs Ferrovial Construction US Corp. and North Perimeter Contractors, LLC

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

FERROVIAL CONSTRUCTION US CORP. and NORTH PERIMETER CONTRACTORS, LLC,	:	CIV. NO. _____
Plaintiffs,	:	JUDGE _____
VERSUS	:	
JESUS GONZALEZ FERNANDEZ.	:	MAGISTRATE _____
Defendants.	:	

VERIFICATION OF FRANCISCO JOSE PALACIOS CLIMENT

I, Francisco Jose Palacios Climent, swear under penalty of perjury that the following is true and correct to the best of my knowledge, information, and belief, which is based on my personal knowledge:

1. I am the Engineering Director for Ferrovial Construction US Corp.

2. I have read the allegations in Paragraphs 14-41 and 47-51 of Plaintiffs' *Verified Complaint for Injunctive Relief and Damages* regarding, for instance, Plaintiffs' business, their efforts to keep business information confidential, the value of the misappropriated information, the harm associated with a competitor having and/or using the misappropriated information, and the investigation into Jesus Gonzalez Fernandez's computing activity.

3. All such allegations are true and correct to the best of my knowledge, information, and belief.

Dated: February 14, 2025

Francisco Jose Palacios _____
Francisco Jose Palacios Climent

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

FERROVIAL CONSTRUCTION US CORP. and NORTH PERIMETER CONTRACTORS, LLC,	:	CIV. NO. _____
Plaintiffs,	:	JUDGE _____
VERSUS	:	
JESUS GONZALEZ FERNANDEZ.	:	MAGISTRATE _____
Defendants.	:	

VERIFICATION OF ERWIN RISHER

I, Erwin Risher, swear under penalty of perjury that the following is true and correct to the best of my knowledge, information, and belief, which is based on my personal knowledge:

1. I am a a Digital Forensic Analyst and Testifying Expert at LCG, LCC "LCG").
2. LCG is a leading provider computer forensic examinations based in Houston, Texas.
3. Plaintiffs retained KCG to assist with the computer forensic analysis of devices used by Jesus Gonzalez Fernandez, with specific focus on his computing activity shortly before his employment ended and any evidence and computing artifacts suggesting the exfiltration of company information.
4. I have read the allegations in Paragraphs 42-46 of Plaintiffs' *Verified Complaint for Injunctive Relief and Damages* regarding computing activity on devices used by Jesus Gonzalez Fernandez.
5. All such allegations are true and correct to the best of my knowledge, information, and belief.
6. A true and correct copy of my CV is attached to this verification as Exhibit 1.

Dated: February 14, 2025

Erin W. Risher

Erwin Risher
Digital Forensic Investigator/Testifying Expert
D 832-852-7895
erisher@lcg-global.com

LCG
Your Partner for Digital Forensics

CURRICULUM VITAE

Mr. Risher is a Digital Forensic Investigator/Testifying Expert at LCG, responsible for the forensic analysis of all types of digital media and technical investigations. Mr. Risher has over 11 years of law enforcement experience with the United States Army Criminal Investigation Command (CID), and over 24 years of experience as a digital forensic examiner, supporting military criminal investigations and corporate employee misconduct/insider risk investigations. Since 2008, Mr. Risher has been an active member of the Scientific Working Group on Digital Evidence (SWGDE) comprised of industry leaders and subject matter experts. SWGDE develops best practices and industry standards for the digital forensics community and is currently serving as Chair of the SWGDE Forensics Committee.

PROFESSIONAL EXPERIENCE

Mr. Risher began his law enforcement career in the U.S. Army in 1994 as a Special Agent for the U.S. Army Criminal Investigation Command (CID). During his 11-year tenure as an enlisted and warrant officer Special Agent, Mr. Risher investigated felony crimes pertaining to active-duty U.S. Army personnel, Department of the Army Civilians, dependent family members, and contractors where there was a U.S. Army interest or significant loss to U.S. Government property and/or funds. He conducted sensitive/serious investigations which included unattended deaths, significant theft of arms, ammunitions, and explosives, homicide and sexual assault. Mr. Risher also collected, analyzed, and disseminated criminal intelligence, conducted and prepared Crime Prevention Surveys and conducted Protective Service Operations as a support person and as a Personal Security Officer for high-ranking U.S. Army and DoD personnel.

During the last three years of Mr. Risher's U.S. Army service, he was selected to be the Assistant Operations Officer and Computer Crimes Coordinator for the Fort Benning CID Battalion. During his tenure, Mr. Risher provided technical guidance to CID Special Agents on the preparation of search and seizure documents, seizure of automation equipment, and shipment of storage media devices for analysis by the Defense Computer Forensics Laboratory, the U.S. Army Criminal Investigation Laboratory (USACIL), or the U.S. Army Computer Crime Investigative Unit. Mr. Risher later deployed to Afghanistan, and he led a team of CID Special Agents.

In 2005, Mr. Risher resigned his commission as a Chief Warrant Officer and became a U.S. Army civilian employee assigned to the U.S. Army Criminal Investigation Laboratory (USACIL) as a Digital Evidence Examiner in which he conducted forensic examinations of computers and digital devices for courtroom quality evidence. Mr. Risher prepared scientific reports of forensics analytical results in clear and understandable language appropriate for courtroom presentation. He rendered expert opinion based on critical and unbiased assessment and analysis of evidence. Additionally, he collaborated with other examiners to develop innovative approaches to conducting forensic examinations. Mr. Risher also conducted training for investigators on best practices for triage of digital devices, seizure of digital evidence, and preparation of legal search authorizations.

In 2016, Mr. Risher exited federal employment and entered the private sector as a Senior Computer Forensics Consultant for Kroll Ontrack, which later became KLDiscovery. Mr. Risher managed and conducted investigations related to data collections, forensic data, file, email analysis, and data recovery within a wide variety of dynamic environments. Additionally, he consulted with key stakeholders to gather requirements, scope the project, and provide consulting solutions for proper data collection, investigations, and reporting. While at KLDiscovery Mr. Risher became the Senior Forensic Analyst, Team Lead, in which he led a team of forensic analysts in conducting digital forensic investigations and analysis.

Exhibit 1

PROFESSIONAL EXPERIENCE (CONT.)

Mr. Risher developed and implemented training programs for team members on new forensic tools and techniques. He collaborated with clients to understand their needs and provide tailored forensic solutions. Additionally, He managed the review process for all forensic analysis results before client delivery. Mr. Risher also identified and recommended new forensic tools and equipment to enhance team capabilities.

In 2018, Mr. Risher joined SunTrust Banks as a Senior Forensic Analyst/Cybersecurity Operations Consultant in which he conducted complex computer forensic examinations in support of internal investigations to ensure protection of intellectual property and client data. Mr. Risher also designed and renovated computer forensic procedures to enhance portability and ease of future updating. Additionally, he developed and implemented forensic processes and procedures based on digital forensics best practices and industry standards. In 2019, after the merger with BB&T Bank, SunTrust and BB&T became Truist, and Mr. Risher was assigned as the Team Lead for Digital Forensics where he led a team of digital forensic examiners, providing guidance and support to junior members while developing and implementing new procedures for evidence handling and chain of custody, which exceeded industry standards. He ensured project objectives were met on time and within budget, maintaining a high level of quality and accuracy and conducted complex computer forensic examinations to protect sensitive data and intellectual property. Additionally, Mr. Risher proactively identified opportunities for process improvements to enhance defensibility and efficiency.

In 2020, Mr. Risher was hired by Carrier Corporation to be the Associate Director, Global Digital Investigation, where he was tasked to create, build, and lead a team providing digital forensics and eDiscovery services within two months after starting the position. He was successful in starting the services on time, but also maturing the services and even adding a Data Loss Prevention (DLP) program and Insider Risk Program. Mr. Risher acted as the main point of contact for forensic investigations regarding insider risks. He also developed relationships and collaborated with key stakeholders (HR, Legal, Data Privacy, Intellectual Property) pertaining to insider risks and data protection.

POSITIONS HELD

- **Digital Forensic Investigator/Testifying Expert** – LCG, Richmond, TX
- **Associate Director, Global Digital Investigation –** Cyber Fusion Center, Cybersecurity, Carrier Corporation, Atlanta, GA (2020 – 2024)
- **Team Lead, Digital Forensics** – Cyber Fusion Center, Cybersecurity, SunTrust Bank now Truist, Atlanta, GA (2019 – 2020)
- **Senior Forensic Analyst/Cybersecurity Operations Consultant** – Cyber Fusion Center, Cybersecurity, SunTrust Bank, Atlanta, GA (2018 – 2019)
- **Senior Forensic Analyst, Team Lead –** KrolLDiscovery/KLDiscovery, Eden Prairie, MN (Remote) (2017 – 2018)
- **Senior Computer Forensics Consultant –** Kroll Ontrack, Eden Prairie, MN (Remote) (2016 – 2017)
- **Digital Evidence Examiner** – U.S. Army Criminal Investigation Laboratory, Atlanta, GA (2005 – 2016)
- **Computer Crimes Coordinator/Assistance Operations Officer** – U.S. Army Criminal Investigation Command (CID), U.S. Army active duty, Fort Benning, GA (2002 – 2005)
- **Special Agent** - U.S. Army Criminal Investigation Command (CID), U.S. Army active duty, various locations (1994 – 2002)

EDUCATION AND CERTIFICATIONS

- Master of Science – Management Information Systems, Bowie State University, Kaiserslautern, Germany
- Bachelor of Arts – Criminal Justice, University of South Alabama, Mobile, AL
- Associate of Science – Pre-Engineering, Jefferson Davis Community College, Brewton, AL
- State of Texas Private Investigator License # 167861401
- EnCase Certified Examiner (EnCE)
- Certified Forensic Computer Examiner (CFCE)
- GIAC Certified Forensic Examiner (GCFE)
- Magnet Certified Forensic Examiner (MCFE)

SELECTED TRAINING

▪ Building an Insider Threat Program, CERT.org (Online)	November 2024
▪ Overview of Insider Threat Concepts and Activities, CERT.org (Online)	November 2024
▪ Magnet AXIOM Advanced Computer Forensics (AX250) (Online)	June 2023
▪ Building an Investigation with EnCase (DF210) (Online)	July 2022
▪ Autopsy 8-Hour Online Training, Basis Technology (Online)	April 2020
▪ Magnet AXIOM Examinations (AX200), Magnet Forensics (Online)	February 2019
▪ Navigating EnCase Forensic V8, Guidance Software (Online)	November 2017
▪ Cellebrite Mobile Forensics Fundamentals (CMFF)	February 2017
▪ Advanced Digital Forensics and Incident Response (FOR508)	November 2015
▪ Internet Evidence Finder 3-day Training Course	June 2015
▪ 5-day Data Recovery Expert Certification Class	June 2015
▪ Windows Forensics Analysis (FOR500)	December 2014
▪ MacIntosh Forensics Training Program	March 2012
▪ EnCase Advanced Internet Investigations	December 2010
▪ MAC Forensics	April 2010
▪ Managing Computer Crime Units	March 2010
▪ Data Recovery	October 2007
▪ Certified Forensic Computer Examiner Course	April 2007
▪ Seized Computer Evidence Recovery Specialist training program	December 2006
▪ EnCase Advanced Computer Forensics	March 2006
▪ EnCase Intermediate Analysis and Reporting	July 2003
▪ Computer Network Investigation Training Program	November 2002

SELECTED TRAINING (CONT.)

- Introduction to Networks and Computer Hardware — October 2000
- Basic Forensic Examinations — April 2000
- Criminal Investigations in an Automated Environment Training Program — September 1997

PROFESSIONAL ASSOCIATIONS

- International Association of Computer Investigative Specialists (IACIS), October 2003 – Present
- Scientific Working Group on Digital Evidence (SWGDE), Forensics Committee, January 2008 – Present

SELECTED SWORN TESTIMONY

Qualified as an expert in Forensic Computer Media Analysis in U.S. Military/Federal Court for the following digital forensic examinations:

- 2011-CID131-1403, Fort Bragg, NC, July 2013
- 2011-CID131-0362, Fort Rucker, AL, July 2012
- 2010-CID131-2013, Schweinfurt, Germany, January 2012
- 2010-CID131-0274, Fort Rucker, AL, March 2011
- 2009-CID131-0877, Fort Stewart, GA, June 2010
- 2008-CID131-0864, Naval Station San Diego, CA, February 2010
- 2008-CID131-0626, Fort Bragg, NC, May 2009
- 2008-CID131-0237, Fort Lee, VA, April 2009
- 2007-CID131-0813, Hanau, Germany, September 2007
- 2007-CID131-0803, Baumholder, Germany, September 2007
- 0066-05-CID083-22443, Montgomery, AL, September 2006
- 2006-CID131-0759, Camp Arifjan, Kuwait, September 2006
- 0303-05-CID013, Fort Stewart, GA, January 2006

Testified as a witness to the fact in U.S. Military/Federal Court for the following digital forensic examinations:

- U.S. v. Frazier (16-ATL-00751), Nashville, TN, July 2022
- 2009-CID131-0667, Fort Wainwright, AK, March 2010
- 2005-CID131-1325, Hanau, Germany, May 2006